In the Claims:

1. (Cancelled)

2. (Currently Amended) A method for intrusion detection of network traffic comprising:

storing a data file comprising data defining one or more signature definition and one or more parameters and associated values;

generating, for each of the one or more signature definitions, an inspector instance based on the data file;

executing, for each of the one or more signature definitions, the generated inspector instance to detect network traffic matching the signature definition;

~~The method of Claim 1, and further comprising:~~

storing a user data file comprising one or more modified signature definitions, each modified signature definition comprising a signature identifier associating the modified signature definition with a corresponding signature definition stored in the data file; and

generating, for each of the modified signature definitions, a revised inspector instance based on the modified signature definition and the corresponding generated inspector instance.

3. (Currently Amended) The method of ~~Claim 1~~ Claim 2, wherein the data file comprises, for each signature definition, data comprising:

a signature identification number parameter and associated value;

a signature name and associated string; and

one or more parameters and respective values defining characteristics of the signature.

4. (Currently Amended) The method of ~~Claim 1~~ Claim 2, wherein each signature definition is stored in a separate line of the data file.

5. (Original) The method of Claim 2, wherein the one or more modified signature definitions comprises modified values for associated modified parameters and no

values indicative of the parameters in the corresponding signature definition that are not modified.

6. (Currently Amended) The method of ~~Claim 1~~ Claim 2, wherein the data file comprises a file received from a sensor provider.

7. (Currently Amended) The method of ~~Claim 1~~ Claim 2, wherein the data file comprises a file generated by a user.

8. (Currently Amended) The method of ~~Claim 1~~ Claim 2, wherein receiving the data file comprises receiving the data file at a sensor configuration handler.

9. (Currently Amended) The method of ~~Claim 1~~ Claim 2, and further comprising receiving configuration data from a user and storing the received configuration data in a user data file.

10. (Currently Amended) The method of ~~Claim 1~~ Claim 2, and further comprising:

storing a user data file comprising one or more user-defined signature definitions, each user-defined signature definition comprising a signature identifier not associated with any of the signature definitions in the data file; and

generating, for each of the user-defined signature definitions, an inspector instance based on the user-defined signature.

11. (Cancelled)

12. (Currently Amended) The method of ~~Claim 11~~ Claim 13, wherein storing a customized signature file comprises storing modifications of one or more of the default signatures.

13. (Currently Amended) A method for use in intrusion detection comprising:

storing a default signature file defining one or more default signatures;

storing a customized signature file defining one or more custom signatures;

automatically generating, for each of the one or more signatures defined in the default signature file, executable code for detecting intrusions associated with the default signature; and

~~The method of Claim 11, wherein automatically generating, for each of the one or more custom signatures comprises~~ automatically generating, for each custom signature, executable code ~~operable to detect~~ for detecting intrusions associated with the custom signature based on the generated executable code of an associated default signature.

14. (Currently Amended) The method of ~~Claim 11~~ Claim 13, wherein the one or more custom signatures comprises modifications of the default signatures.

15. (Currently Amended) The method of ~~Claim 11~~ Claim 13, wherein generating, for each of the one or more default signatures, comprises generating executable code associated with the default signature based on an inspector shell.

16. (Currently Amended) The method of Claim 15, wherein the executable code associated with the default signature ~~is operable to compare~~ compares a plurality of parameter values to a plurality of parameter values defined by the default signature.

17. (Currently Amended) The method of ~~Claim 11~~ Claim 13, wherein the default signature file comprises, for each default signature;

a signature identification number parameter and associated value;

a signature name and associated string; and

one or more parameters and respective values defining characteristics of the default signature.

18. (Currently Amended) The method of ~~Claim 11~~ Claim 13, wherein the custom signature file comprises, for each signature:

a signature identification number parameter and associated value;

a signature name and associated string; and

one or more parameters and respective values defining characteristics of the default signature.

Claims 19 - 39 (Cancelled)